



# **NetCamera NVW IP Security Wireless Night Vision Camera A02-IPCAM4-W54**



**MANUAL**  
**A02-IPCAM4-W54\_ME01**

**Where solutions begin**



### ITALIANO

Questo prodotto è coperto da garanzia Atlantis Land **Fast-Swap** della durata di 3 anni. Per maggiori dettagli in merito o per accedere alla documentazione completa in Italiano fare riferimento al sito [www.atlantis-land.com](http://www.atlantis-land.com).

### ENGLISH

This product is covered by Atlantis Land 3 years **Fast-Swap** warranty. For more detailed informations please refer to the web site [www.atlantis-land.com](http://www.atlantis-land.com). For more detailed instructions on configuring and using this device, please refer to the online manual.

### FRANCAIS

Ce produit est couvert par une garantie Atlantis Land **Fast-Swap** de 3 ans. Pour des informations plus détaillées, référez-vous svp au site Web [www.atlantis-land.com](http://www.atlantis-land.com).

### DEUTSCH

Dieses Produkt ist durch die Atlantis Land 3 Jahre **Fast-Swap** Garantie gedeckt. Für weitere Informationen, beziehen Sie sich bitte auf Web Site [www.atlantis-land.com](http://www.atlantis-land.com).

### ESPAÑOL

Este producto esta cubierto por Atlantis Land con una garantía **Fast-Swap** de 3 años. Para mayor información diríjase a nuestro sitio Web [www.atlantis-land.com](http://www.atlantis-land.com).



The award of the information is facultative, but its lack will prevent ATLANTIS LAND® from starting the Guarantee process requested.



**Register your product!**

**[www.atlantis-land.com](http://www.atlantis-land.com)**

Registration on the web site **[www.atlantis-land.com](http://www.atlantis-land.com)** within 15 days from the purchase of the product dismiss the customer from showing a valid proof of purchase (Sale Receipt or Invoice) in case of the request of intervention. For further information we invite you to look at our web site at the section WARRANTY.

### **Copyright**

The Atlantis Land logo is a registered trademark of Atlantis Land S.p.A. All other names mentioned may be trademarks or registered trademarks of their respective owners. Subject to change without notice. No liability for technical errors and/or omissions.



# INDEX

Chapter 1 .....	9
1.1 An Overview of NetCamera NVW .....	9
1.2 System Requirements .....	10
1.3 Package Contents .....	10
Chapter 2 .....	11
2.1 Cautions for NetCamera NVW .....	11
2.2 The Front LEDs .....	12
2.3 The Rear Ports .....	14
2.4 Assembling the Stand and Connecting to a Network .....	16
Chapter 3 .....	18
3.1 Before Configuration .....	18
3.1.1 Windows 95/98/ME .....	19
3.1.2 Windows NT4.0 .....	19
3.1.3 Windows 2000 .....	19
3.1.4 Windows XP .....	20
3.2 Default Settings .....	20
3.3 Browser configuration .....	21
Chapter 4 .....	24
4.1 Basic Settings .....	27
4.1.1 System .....	27
Status .....	28
Log .....	29
Time .....	30
Firmware .....	31
4.1.2 Network .....	33
Ethernet .....	34
Wireless .....	36
PPPoE .....	41
DDNS .....	42
4.1.3 User .....	43
User .....	43
Password .....	43



4.1.4 Video .....	44
Video .....	45
Audio .....	47
4.1.5 Video Player .....	48
4.2 Advanced .....	49
4.2.1 FTP .....	49
4.2.2 Mail .....	50
4.2.3 GPIO .....	51
4.2.4 Breach Manager .....	52
Chapter 5 .....	54
5.1 Support .....	54
APPENDIX A: Frequently Asked Questions .....	55
A.1 Using LEDs to Diagnose Problems .....	55
A.1.1 LED Power .....	55
A.1.2 LED LAN .....	55
A.2 WEB .....	56
A.3 Login .....	56
A.4 General Questions .....	57
APPENDIX B: Trouble Shooting .....	62
APPENDIX C: Adjusting the Camera Focus .....	67
APPENDIX D: GPIO .....	68
APPENDIX E: Glossary of Terms .....	74
APPENDIX F: Technical Features .....	83

**A02-IPCAM4-W54\_ME01(V1.0 December 2006)**



### **Copyright Statement**

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise without the prior writing of the publisher. Windows™ 98SE/2000/ME/XP are trademarks of Microsoft® Corp. Pentium is trademark of Intel. All copyright reserved.

The Atlantis Land logo is a registered trademark of Atlantis Land SpA. All other names mentioned may be trademarks or registered trademarks of their respective owners. Subject to change without notice. No liability for technical errors and/or omissions.

### **Wireless LAN, Health and Authorization for use**

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions however are far much less than the electromagnetic energy emissions from wireless devices like for example mobile phones. Wireless LAN devices are safe for use frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments for example:

- On board of airplanes, or
- In an explosive environment, or
- In case the interference risk to other devices or services is perceived or identified as harmful

In case the policy regarding the use of Wireless LAN devices in specific organizations or environments (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.) is not clear, please ask for authorization to use these devices prior to operating the equipment.

### **Regulatory Information/disclaimers**

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The Manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, of the substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

**CE Mark Warning**

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

**CE in which Countries where the product may be used freely:**

Germany, UK, Italy, Spain, Belgium, Netherlands, Portugal, Greece, Ireland, Denmark, Luxembourg, Austria, Finland, Sweden, Norway and Iceland.

France: except the channel 10 through 13, law prohibits the use of other channels.

**CE/EMC Restriction of Liability**

The product described in this handbook was designed, produced and approved according to the EMC-regulations and is certified to be within EMC limitations.

If the product is used in an uncertified PC, the manufacturer undertakes no warranty in respect to the EMC limits. The described product in this handbook was constructed, produced and certified so that the measured values are within EMC limitations. In practice and under special circumstances, it may be possible, that the product may be outside of the given limits if it is used in a PC that is not produced under EMC certification. It is also possible in certain cases and under special circumstances, which the given EMC peak values will become out of tolerance. In these cases, the user himself is responsible for compliance with the EMC limits.

**Declaration of Conformity**

This equipment has been tested and found to comply with Directive 1999/5/CE of the European Parliament and of the Council on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity. After assessment, the equipment has been found to comply with the following standards: EN 300.328 (radio), EN 301 489-1, EN 301 489-17 (electromagnetic compatibility) and EN 60950 (safety). This equipment may be used in all European Union countries and in all countries applying Directive 1999/5/CE, without restriction, with the exception of the following countries:

**France:** When this equipment is used outdoors, output power is limited to within the frequency bands listed on the chart. For more info, consult the website [www.art-telecom.fr](http://www.art-telecom.fr).

Location	Frequency Band (MHz)	Power (EIRP)
Indoor (no restriction)	2400-2483,5	100mW(20dBm)
Outdoor	2400-2454	100mW(20dBm)
	2454-2483,5	10mW(10dBm)

**Italy:** For more info, consult the website [www.comunicazioni.it](http://www.comunicazioni.it)



# Chapter 1

## Introduction

This manual is think for an advanced utilization of NetCamera NVW; for this reason, you can find explanation of any functions supported by product. For fast configuration, please referee to Quick Start Guide.

### 1.1 An Overview of NetCamera NVW

NetCamera NVW is the ideal solution for sending videos, remote video surveillance and for the transmission of images in real-time over your Intranet or the Internet.

NetCamera NVW is equipped with a powerful CPU and integrates the robust Linux operating system enabling to integrate, among its many features, automatic movement detection via hardware in MPEG4 format with VGA resolution and constant rates of 30 fps; recording not only the video but also the sound.

Its back panel contains 3 pairs of connectors (2 input and 1 output) allowing the camera to communicate with different elements of a building, such as electric doors and light switches or security related devices such as alarms.

Furthermore, thanks its 8 integrated Infrared sensors, the NetCamera NVW's automatic Day/Night functionality will change to Infrared mode as it becomes dark, providing a video quality on par with its daylight settings.

Its ability to see in the dark as well as the integrated motion detection functionality, turn this camera into the ideal device for remote video surveillance night and day; even when there is no light.

NetCamera NVW can be connected, via network cable, directly to the LAN or it can use the wireless interface in IEEE802.11g standard with the support of the highest security standards.

Using the web browser of any PC or notebook connected to the Internet (or Intranet), the NetCamera NVW provides the user with a highly intuitive interface to manage and control it remotely, making it the ideal tool for remote monitoring and video surveillance.





## 1.2 System Requirements

Before installing the device, your PC should meet the following:

- Local Area Network: 10Base-T Ethernet or 100Base TX Fast Ethernet
- CPU: Intel Celeron 1.5GHz or above (Intel Pentium 4 is preferred)
- Memory Size: 128 MB (256 MB recommended)
- VGA card resolution: 800x600 or above
- Internet Explorer 5.0 or above (ActiveX)

## 1.3 Package Contents

Unpack the package and check all the items carefully. If any item contained is damaged or missing, please contact your local dealer as soon as possible. Also, keep the box and packing materials in case you need to ship the unit in the future. The package should contain the following items:

- One IP Security Wireless Night Vision Camera
- One Quick Installation Guide
- One Installation CD Rom with Manuals and Utility
- One Metal Clip (wall mounting).
- One DC Power Adapter
- One RJ-45 Ethernet Cable

**If any of the above items are missing, please contact your reseller.**

## Chapter 2

### Using NetCamera NVW

#### 2.1 Cautions for NetCamera NVW

Read this section to learn how to set up your IP camera and use its basic functions.



Do not place the NetCamera NVW under high humidity and high temperature. It can damage the device.

Do not use the same power source for NetCamera NVW with other equipment.

Do not open or repair the case yourself.

If the NetCamera NVW is too hot, turn off the power immediately and have a qualified serviceman repair it.



Ensure the camera is fixed securely otherwise it may fall and cause injury.

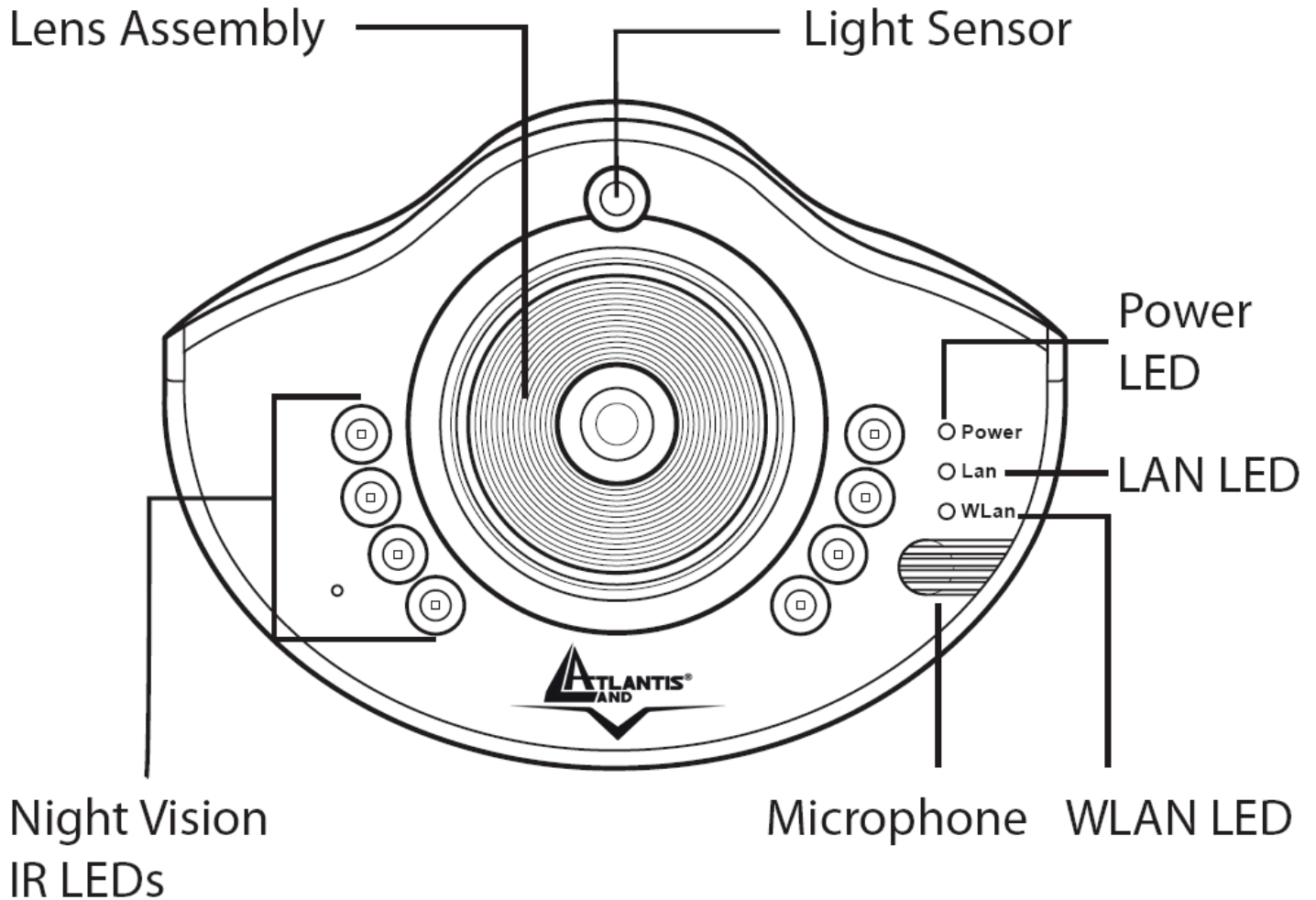
The camera is not waterproof and should not be mounted outside or in a position where it could become wet.

Place the NetCamera NVW on a stable surface.

Only use the power adapter that comes with the package.

Do NOT upgrade firmware on any Atlantis Land product over a wireless connection. Failure of the device may result. Use only hard-wired network connections.

## 2.2 The Front LEDs



LED	Meaning
Power	Lights when power ON
Lan	Network activity indicator Flashes when sending/receiving data
WLAN	Network activity indicator Flashes when sending/receiving data

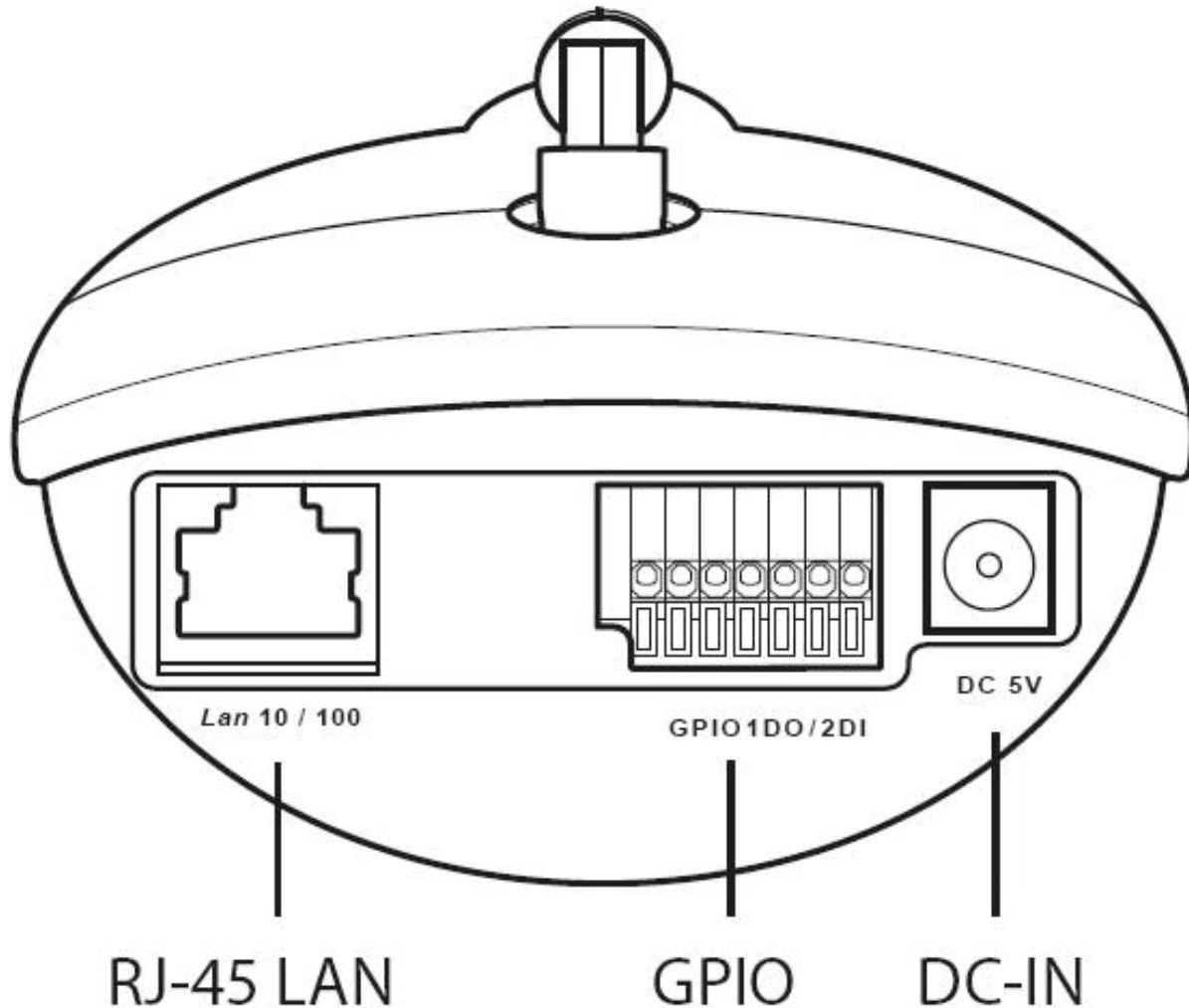


<b>Night Vision</b>	Furthermore, thanks its 8 integrated Infrared sensors, the NetCamera NVW's automatic Day/Night functionality will change to Infrared mode as it becomes dark
<b>Light Sensor</b>	Light Sensor (Don't cover this Led)
<b>Microphone</b>	Microphone for environmental sound recording



Use of audio or video equipment for recording the image or voice of a person without their knowledge and consent is prohibited in certain states or jurisdictions. Nothing herein represents a warranty or representation that the Atlantis product provided herein is suitable for the end-user's intended use under the applicable laws of his or her state. Atlantis disclaims any liability whatsoever for any end-user use of the Atlantis product, which fails to comply with applicable state, local, or federal laws.

## 2.3 The Rear Ports

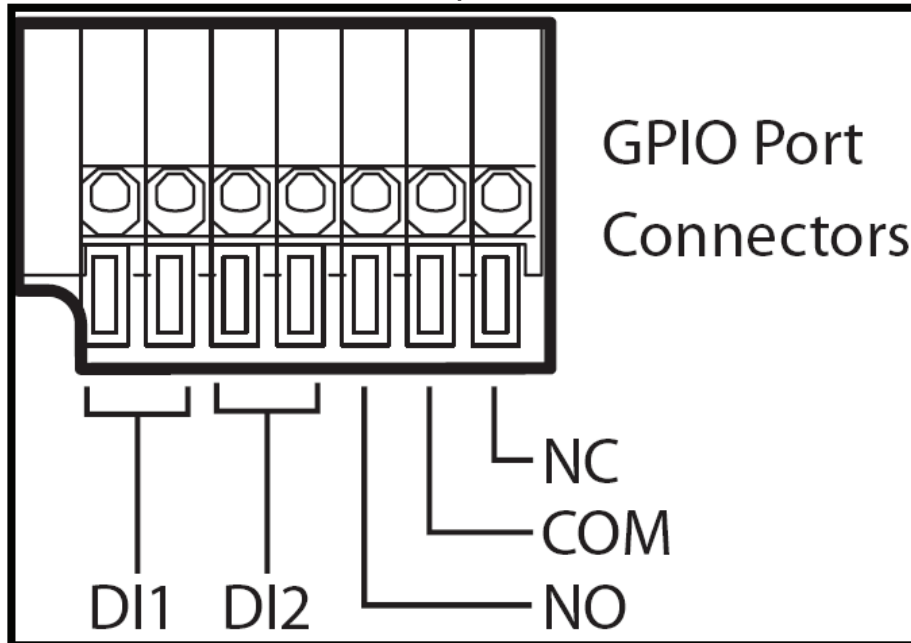


Port	Meaning
<b>Network Cable</b>	Ethernet port with 10/100Mbps Fast Ethernet connections, connect this port to switch/hub
<b>GPIO Connectors</b>	Its back panel contains 3 pairs of connectors (2 x DI input and 1 x DO output)

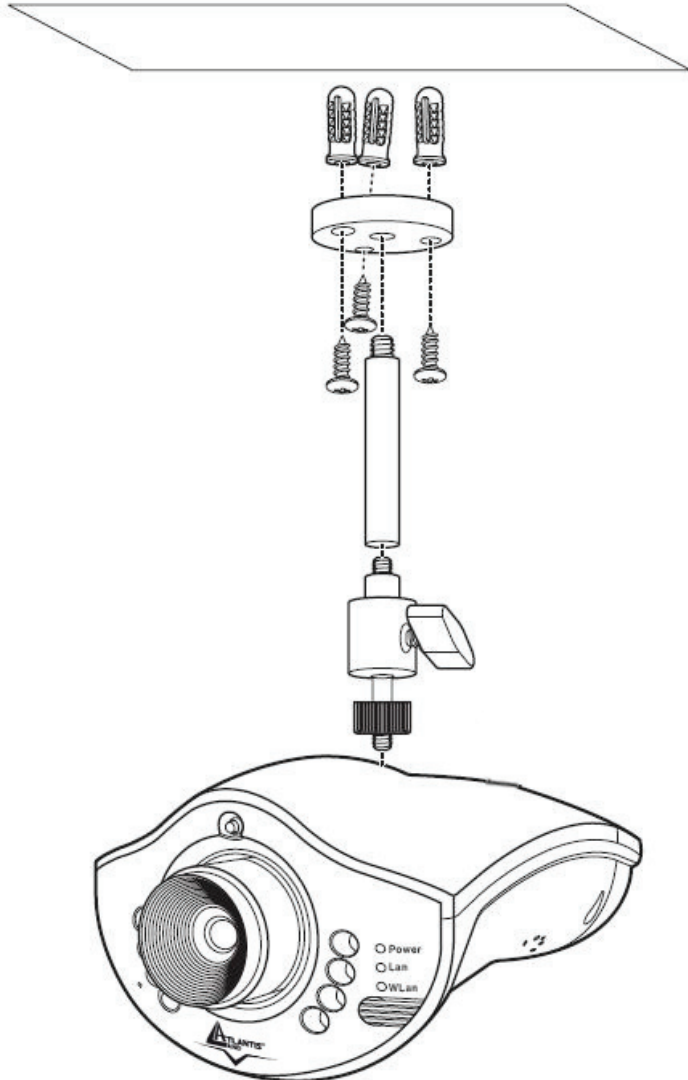


DC-IN	Connect the Power Adapter DC plug to the AP's power jack
-------	--

Please check the attached picture in order to obtain more info about GPIO port.



## 2.4 Assembling the Stand and Connecting to a Network



The camera can be assembled in two different ways; either from the top of the unit or the bottom. Assemble the stand and fix it to the camera as shown.

Use the three screws and plugs provided to fix the stand bracket to a wall, ceiling or other convenient fixing point.

The stand can be adjusted to allow the camera a full 360° of rotation and a pan and tilt action.

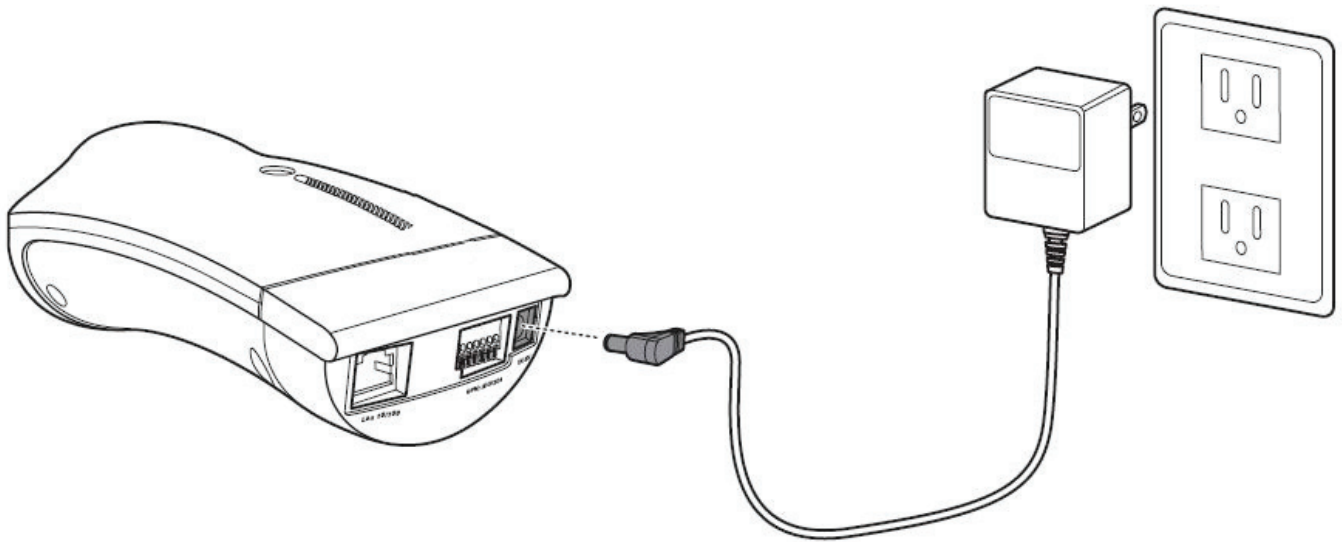
Follow the above steps to mount from the base of the unit, attaching the stand bracket to the mounting point on the base of the unit.



Ensure the camera is fixed securely otherwise it may fall and cause injury.

The camera is not waterproof and should not be mounted outside or in a position where it could become wet.

Connect the power adapter to the DC-IN socket on the camera as shown then check Power Led.



The IP camera can be connected to an Ethernet network using the RJ-45 port as shown. Connect the camera to an Ethernet hub or switch using a standard cable. You can also connect the camera directly to a computer using the supplied cable.

**NOTE:**  


Use only the power adapter with the camera. Using another adapter, not recommended by the manufacturer, may damage the camera and invalidate the warranty.





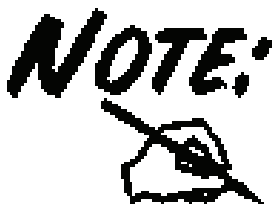
## Chapter 3

### Configuration

The NetCamera NVW can be configured with your Web browser. The web browser is included as a standard application in the following operation systems, UNIX, Linux, Mac OS, Windows 95/98/NT/2000/Me, and etc. The product provides a very easy and user-friendly interface for configuration.

#### 3.1 Before Configuration

This section describes the configuration required by LAN-attached PCs that communicate with the NetCamera NVW, either to configure the device or for network access. These PCs must have an Ethernet interface installed properly, be connected to the Router either directly or through an external repeater hub, and have a fixed IP address that must be in the same subnet of the NetCamera NVW. The default IP address of the NetCamera NVW is 192.168.1.1 and subnet mask is 255.255.255.0. Please follow the steps below for PC's network environment installation. First of all, please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to MS Windows related manuals.



Any TCP/IP capable workstation can be used to communicate with or through the NetCamera NVW. To configure other types of workstations, please consult the manufacturer's documentation.



### 3.1.1 Windows 95/98/ME

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.
2. Select **TCP / IP -> NE2000 Compatible**, or the name of any Network Interface Card (NIC) in your PC.
3. Click **Properties**.
4. Select the **IP Address** tab. In this page, click the **Specify an IP address** radio button (EG IP=192.168.1.2 and subnet Mask=255.255.255.0).

### 3.1.2 Windows NT4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Protocols** tab.
2. Select **TCP/IP Protocol** and click **Properties**.
3. Select the **IP Address** tab. In this page, click the **Specify an IP address** radio button (EG IP=192.168.1.2 and subnet Mask=255.255.255.0).

### 3.1.3 Windows 2000

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.
2. Double-click **LAN Area Connection**.
3. In the **LAN Area Connection Status** window, click **Properties**.
4. Select **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select **Use the Following IP Address** (EG IP=192.168.1.2 and subnet Mask=255.255.255.0).
6. Click **"OK"** to finish the configuration.



### 3.1.4 Windows XP

1. Go to **Start / Control Panel** (in Classic View). In the Control Panel, double-click on **Network Connections**.
2. Double-click **Local Area Connection**
3. In the LAN Area Connection Status window, click Properties.
4. Select **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select the **Use the following IP address** radio buttons (EG IP=192.168.1.2 and subnet Mask=255.255.255.0).
6. Click **“OK”** to finish the configuration.

### 3.2 Default Settings

Before you configure this NetCamera NVW, you need to know the following default settings:

- **Password: admin**
- **Username: atlantis**
- **Indirizzo IP: 192.168.1.1**
- **Subnet Mask(255.255.255.0)**
- **Wireless:**
  - Connection Type=Infra
  - Contry Region=ETSI(Europe)
  - Channel=6
  - SSID(ESSID)=NetCameraNVW

### 3.3 Browser configuration

Open the web browser, enter the local port IP address of this NetCamera NVW, which default at **192.168.1.1**, and click “Go” to get the login page.



At the configuration homepage, the left navigation pane where bookmarks are provided links you directly to the desired setup page, including:

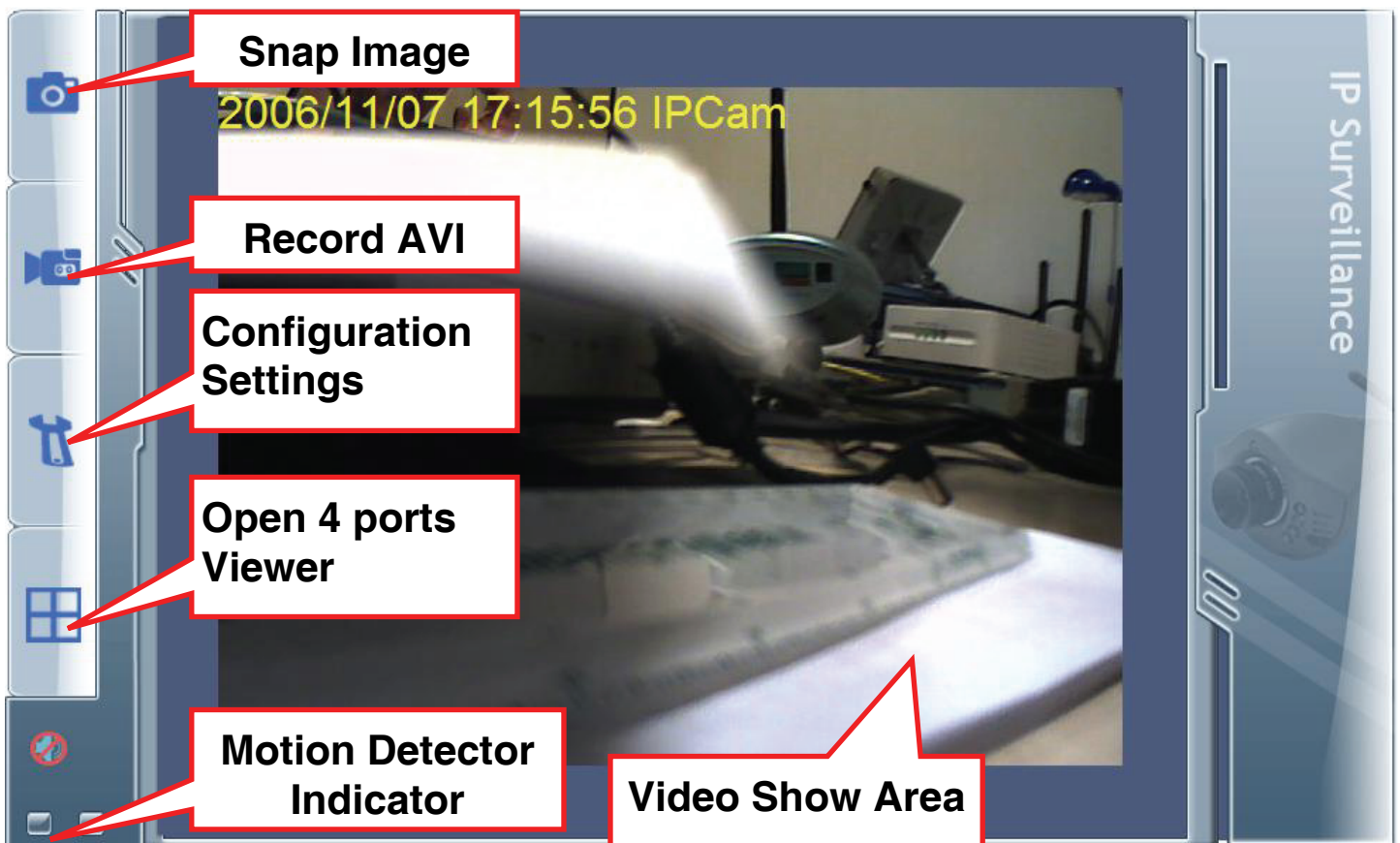
**NOTE:**

Please refer to the appendix on how to install ActiveX.  
Please refer to the appendix on how to install ActiveX.

- At the top click **This site might require the following ActiveX Control: 'ATL3.0:VCView' from 'Atlantis Land SpA' . Click here to**

### install....

- Click **Install ActiveX Control....**
- In the *Security Warning* window click **Install**.
- The live video will now be streamed.



Use the menu bar on the left side of the screen to perform actions and enter the sub-menus:

- **Snap Image:** Click to save the current image.
- **Record AVI:** Click to record an AVI video clip.
- **Configuration Settings:** Click to enter the settings sub-menus.
- **Open 4 ports View:** Click to view the output of up to four other IP cameras on the network.

For more detailed instructions on configuring and using the NetCamera NVW, please refer to the online manual.



The computer's IP address must correspond with the camera's IP address in the same segment for the two devices to communicate (E.G. IP=192.168.1.2 and Subnet Mask=255.255.255.0).



## Chapter 4

### Advanced Configuration

Read this chapter to learn how to operate the IP camera and take advantage of the advanced features such as alerting, and ftp transfers.

Open the web browser, enter the local port IP address of this NetCamera NVW, which default at **http://192.168.1.1**, and click “Go” to get the login page.



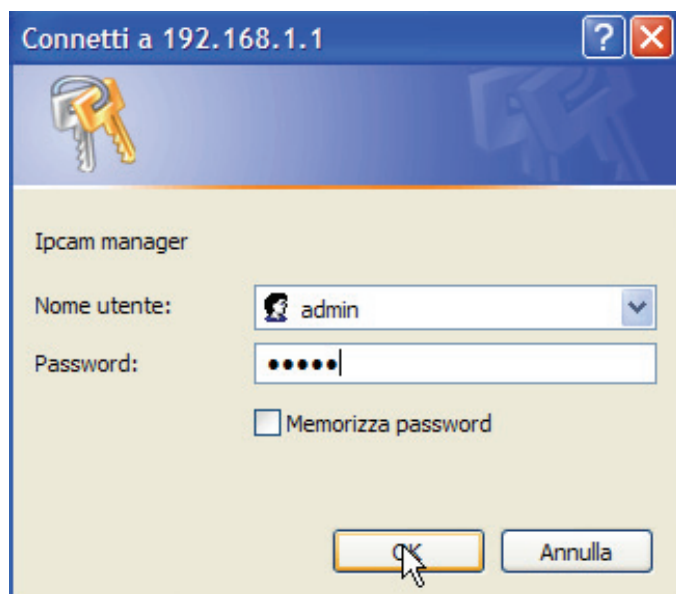
Please refer to the appendix on how to install ActiveX.

To access the settings menus, do the following:



Click the button on the menu sidebar.

A login prompt appears:





Enter your User Name and password. The default are **admin / atlantis**.



The computer's IP address must correspond with the camera's IP address in the same segment for the two devices to communicate.

If you are denied to enter the Web Configuration Utility, the following warning message will appear on the screen. Please try to enter the correct username and password again, or contact your network administrator.





There are 3 sub menus in the menu sidebar: Home, Basic Setting and Advanced Setting.

The screenshot shows the NetCamera NVW web interface. On the left is a menu sidebar with three main sections: Home (represented by a house icon), Basic (represented by a wrench icon), and Advanced (represented by a screwdriver icon). The Basic section is currently selected. The main content area displays the 'Basic Settings' page. At the top of this page is a 'System' menu with sub-items: System, Network, User, Video, and Video Player. Below this is a 'Camera Name' field with the value 'IPCam-5C24' and a 'Save' button. Further down is a 'Wireless Status' section with the following details:

Wireless Status	
Connection	DOWN
Channel	1
Signal Level	0%
TX Rate	54Mbps



## 4.1 Basic Settings

Read this section to learn about all the settings and options under the Basic Setting sub menu. There are five main screens, accessed via the tabs at the top of the screen:

- System
- Network
- User
- Video
- Video Player

### 4.1.1 System

The System submenu allows you to configure all system-related settings. There are four main screens, accessed via the tabs at the top of the screen:

- Status
- Log
- Time
- Firmware



## Status

Click the **Status** tab to access the system status screen:

Status	Log	Time	Firmware
<b>Camera Information</b>			
Firmware Version	C64000-WX-2.00.00-60728-ZZ		
Camera Type	CMOS		
Current Live-View Users	0		
Camera Name	<input type="text" value="IPCam-5C24"/>		<input type="button" value="Save"/>
<b>Ethernet Status</b>			
Ethernet MAC Address	00-14-29-00-5C-24		
LAN IP Address	192.168.1.186		
LAN Netmask Address	255.255.255.0		
LAN Gateway Address	192.168.1.6		
DHCP State	Disabled		
<b>Wireless Status</b>			
Connection	DOWN		
Channel	1		
Signal Level	0%		
TX Rate	54Mbps		

Here is displayed all camera, ethernet and wireless status information, including firmware version and camera name and type.



## Log

Click the **Log** tab to access the log list screen.

**Status** **Log** **Time** **Firmware**

**Log List**

Time	Event
001 11:20:18 11/16/2006	Connect to LiveView
002 10:29:07 11/16/2006	guest login in from 192.168.1.185
003 10:29:06 11/16/2006	admin login in from 192.168.1.185
004 10:26:52 11/16/2006	guest login in from 192.168.1.185
005 10:26:51 11/16/2006	admin login in from 192.168.1.185
006 10:16:43 11/16/2006	guest login in from 192.168.1.185
007 10:16:42 11/16/2006	admin login in from 192.168.1.185
008 10:16:11 11/16/2006	Connect to LiveView
009 10:16:06 11/16/2006	guest login in from 192.168.1.185
010 09:39:54 11/16/2006	guest login in from 192.168.1.185

**Clear** **PrePage** **NextPage**

Here you can view a log of all recent system activity. Click the **PrePage** and **NextPage** buttons to move to the previous or next page of the log and the **Clear** button to clear the log list.



## Time

Click the **Time** tab to access the date and time settings screen.

Status	Log	Time	Firmware
--------	-----	------	----------

### Current Camera Time

Date:  Time:

### NTP Configuration

☒ Synchronize with Time server

Time Zone

NTP server

### Manually Update Camera Time

Synchronize with computer time

Date:  Time:

Set manually

Date:  Time:

Choose to either **Synchronize with Time Server**, **Synchronize with computer time** or **Set manually**.

If you select **Synchronize with Time Server**, check the check-box, choose your time zone, and enter NTP server details. Click the **Save** button to save your settings and the **Refresh** button to update the system date and time.

If you choose **Synchronize with computer time**, the current time displayed by your PC is shown. Click the **Update** button to update the system date and time.

If you choose **Set manually**, enter the the date and time manu-ally and click the **Update** button.



If You meet problems, please follow these instructions:

**NTP Server=pool.ntp.org or 128.138.140.44**

Click the **Save** button to save your settings and the **Refresh** button to update the system date and time.

## Firmware

Click the **Firmware** tab to access the firmware upgrade screen:

Here you can upgrade the system firmware version, reset and restore original camera settings.

Status	Log	Time	Firmware
<b>Maintain Camera</b>			
<input type="button" value="Restart"/> Restart camera.			
<input type="button" value="Restore"/> Reset all parameters, except IP address configuration, to original factory settings.			
<input type="button" value="Default"/> Reset all parameters to original factory settings.			
<b>Upgrade Firmware</b>			
Current version: C64000-WX-2.00.00-60728-ZZ			
<b>Warning: Do not unplug camera power while upgrading.</b>			
Specify the firmware file to upgrade:			
<input type="text"/> <input type="button" value="Sfoglia..."/> and click <input type="button" value="Upgrade"/>			
It will restart automatically after 2 minutes.			

Click the **Restart** button to restart the camera.

Click the **Restore** button to reset all parameters, except IP address configuration, to original factory settings.

Click the **Default** button to reset all parameters to original factory settings.



Click the **Sfogliala(Browse)** button and locate the folder where the firmware update is stored. Click the **Upgrade** button to upgrade the firmware.



Do NOT upgrade firmware on any Atlantis Land product over a wireless connection. Failure of the device may result. Use only hard-wired network connections.

After upgrading you must reset the router to factory default settings, then manually re-enter your settings.

Please pay attention. In case electrical shutdown, during this procedure, this product could be not usable.

When uploading software to the NetCamera NVW, it is important not to interrupt the Web browser by closing the window or loading a new page. If the browser is interrupted, it may corrupt the software.





### 4.1.2 Network

The **Network** submenu allows you to configure all system-related settings. There are four main screens, accessed via the tabs at the top of the screen:

- Ethernet
- Wireless
- PPPoE
- Dynamic DNS





## Ethernet

Click the **Ethernet** tab to access the ethernet settings screen:

Ethernet	Wireless	PPPoE	DDNS
<b>IP Configuration</b>			
<input type="radio"/> Obtain IP address via DHCP <a href="#">View</a>			
<input checked="" type="radio"/> Use the following IP address:			
IP Address	<input type="text" value="192.168.1.1"/>		
Subnet Mask	<input type="text" value="255.255.255.0"/>		
Default Gateway	<input type="text" value="192.168.1.6"/>		
<b>DNS Configuration</b>			
<input type="radio"/> Obtain DNS server address via DHCP <a href="#">View</a>			
<input checked="" type="radio"/> Use the following DNS server address:			
Primary DNS server	<input type="text" value="192.168.1.211"/>		
Secondary DNS server	<input type="text"/>		
<b>HTTP Port</b>			
HTTP port:	<input type="text" value="80"/>		
<a href="#">Save</a> <a href="#">Reload</a>			

Here you can configure all settings related to your ethernet, wireless, and DNS & HTTP port setup.

Under **IP Configuration** and **DNS Configuration**, either enter the settings manually or select the **Obtain IP address via DHCP** and **Obtain DNS server address via DHCP** radio button to obtain the addresses via DHCP. Click the **View** button to view all settings allocated via DHCP.

Click the **Save** button to save your settings. Click the **Reload** button to clear all fields and reload the page.

**HTTP Port:** This is the port number the router's embedded web server (for web-based configuration) will use. The default value is the standard HTTP port, 80. Users may



specify an alternative if, for example, they are running a web server on a PC within their LAN.

For Example: User A changes HTTP port number to 8081. The NetCamera NVW will only allow User A access typing: <http://192.168.1.1:8081> in their web browser.



## Wireless

Click the **Wireless** tab to access the wireless settings screen:

Ethernet	Wireless	PPPoE	DDNS
<b>Basic Configuration</b>			
Connection Type:		Infra ▼	
Country Region:		ETSI ( Europe ) ▼	
Channel:		6 ▼	
SSID (ESSID):		NetCameraNV	
Ad-Hoc Type:		802.11g 54Mbps ▼	
<b>Security Configuration</b>			
Authentication Type:		Open System ▼	
Encryption Type:		None ▼	
WEP Key :		<input type="text"/> ( 5, 10, 13, 26 letters )	
<input type="button" value="Save"/>		<input type="button" value="Reload"/>	

- **Connection Type:** Use this option to determine the type of wireless communication for the camera. There are two choices: **Infrastructure** mode and **Ad-Hoc** mode.
- **Country Region:** For some European Country, it may have its own domain; users are responsible for ensuring that the channel set configuration is in compliance with the regulatory standards of these countries.
- **Channel:** This pull-down menu provides the wireless channel for communication. A “channel” is a range of frequencies to be used in communication between the camera and access point in Infrastructure mode, or the camera and PC/Notebook in Ad-Hoc mode. Select the appropriate channel from the list provided depending on the regulatory region where the unit is sold.
- **SSID:** SSID (Service Set Identity) is the name assigned to the wireless network. It will auto-detect and display the SSID of wireless network



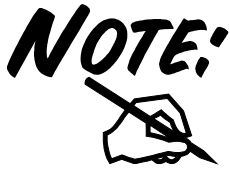
connected in this box. This default setting will let the camera connect to ANY access point under the infrastructure network mode.

- **Ad-Hoc Type:** Please select between **802.11g** or **802.11b** if You are using a AD-Hoc network.

**Security Configuration:** Wireless network communications can be intercepted easily. This option will help you protect your wireless network.

- **Authentication: Open** communicates the key across the network. **Shared** allows communication only with other devices with identical WEP settings. **WPA-PSK** You have to insert a KEY.
- **Encryption Type:** This option allows you to configure the setting of data encryption. The WEP/WPA key must be set before the data encryption is enforced.
- **WEP KEY/WPA-PSK KEY:** To enable WEP Encryption, you should decide the encryption format first by selecting the **ASCII** or **HEX** option, and then input the WEP key (in the following **Key 1~4** box). To enable WPA Encryption, you have to insert directly the key (minimum 8 characters). **Pre-Shared Key:** This is used to identify each other in the network. Enter the name in the **Pre-Shared Key** box, and this name must match the Pre-Shared Key value in the remote device. You can check in the picture an example of configuration in WPA-PSK.

Ethernet	Wireless	PPPoE	DDNS
<b>Basic Configuration</b>			
Connection Type:		Infra	
Country Region:		ETSI (Europe)	
Channel:		1	
SSID (ESSID):		A02-AP2-W54M	
Ad-Hoc Type:		802.11g 54Mbps	
<b>Security Configuration</b>			
Authentication Type:		WPA-PSK	
Encryption Type:		TKIP (WPA-PSK)	
WEP Key :		<input type="text"/> ( 5, 10, 13, 26 letters )	
WPA-PSK Key :		<input type="text" value="stefanino7791"/>	
<input type="button" value="Save"/>		<input type="button" value="Reload"/>	

**How to configure WEP security:**

If you select 64bit in Hex format, you must type 10 values in the following range (0~F, hexadecimal), or 64bit in ASCII format, you must type 5 values in the following range (0~9, A~Z and a~z Alphanumeric).

If you select 128bit in Hex format, you must type 26 values (0~F, hexadecimal), or 128bit in ASCII format, you must type 13 values in the following range (0~9, A~Z and a~z Alphanumeric).

	ASCII	HEX
64 bit	5*X	10*Y
128 bit	13*X	26*Y

X=[(0~9, A~Z, a~z Alphanumeric)]

Y=[0~9, A~F Hexadecimal]

Be sure that the NetCamera NVW and the wireless station (AP) were set in the same key.



WEP is not completely secure. If possible please use WPA-PSK.



**Ad-hoc Mode:** An Ad-hoc network is a local area network or other small network, especially one with wireless or temporary plug-in connections, in which some of the network devices are part of the network only for the duration of a communications session. Users in the network can share files, print to a shared printer, and access the Internet with a shared modem. In this kind of network, new devices can be quickly added; however, users can only communicate with other wireless LAN computers that are in this wireless LAN workgroup, and are within range.

**Infrastructure Networking Mode:** The difference between Infrastructure network and Ad-hoc network is that the former one includes an Access Point. In an Infrastructure network, the Access Point can manage the bandwidth to maximize

bandwidth utilization. Additionally, the Access Point enables users on a wireless LAN to access an existing wired network, allowing wireless users to take advantage of the wired networks resources, such as Internet, email, file transfer, and printer sharing. The scale and range of the Infrastructure networking are larger and wider than that of the Ad-hoc networking.



The range of radio frequencies used by IEEE 802.11g wireless devices is called a “channel”. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.



For some European Country, it may have its own domain; users are responsible for ensuring that the channel set configuration is in compliance with the regulatory standards of these countries.

You can check under **System-Status** the status/quality of wireless Link.



#### Wireless Status

Connection	UP
Channel	1
Signal Level	100%
TX Rate	54Mbps







## PPPoE

Click the **PPPoE** tab to access the PPPoE settings screen:

**Ethernet** **Wireless** **PPPoE** **DDNS**

Configuration

☒ Enable PPPoE

User Name:

Password:

☒ Send Email when IP change

Status

IP Address: 0.0.0.0

Default Router: 0.0.0.0

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

Connection State: Disabled

Here you can configure all PPPoE connection settings. If you connect to your network via PPPoE, check the **Enable PPPoE** checkbox and enter your User Name and password. Check the **Send Email when IP change** checkbox if you wish to be notified of any IP change via email. Click the **Save** button to save all changes. The system will begin to connect via PPPoE. Click the **Reload** button to reload the page. Status details are displayed under Status. Click the **Refresh** button to update these details at any time.

Dynamic DNS client can work correctly only if PPPoE is activated.







## DDNS

Click the **DDNS** tab to access the DDNS settings screen:

Here you can configure all DDNS connection settings.

DDNS allows PPPoE or DHCP dynamic IP users to access the IP camera using a single domain name. The IP camera supports DDNS and meets the Dynamic Network Service, Inc. standard. Select the DDNS server type: Disabled, DynDNS, or PeanutHull.

Ethernet	Wireless	PPPoE	DDNS
Dynamic DNS			
DDNS Server <input type="radio"/> Disabled <input checked="" type="radio"/> DynDNS <input type="radio"/> PeanutHull			
Hostname (Domain): <input type="text"/>			
Username (Passport): <input type="text"/>			
Password: <input type="text"/>			
Status:			
<input type="button" value="Save"/> <input type="button" value="Reload"/>			

Click the **Save** button to save your settings. Click the **Reload** button to clear all fields and reload the page.



When the IP address of the camera changes, it will update its new address to DDNS automatically and the camera can be contacted using a domain name instead of an IP address. DNS status is displayed under **Status**.



Dynamic DNS client can work correctly only if PPPoE is activated.



### 4.1.3 User

The User submenu enables you to set up users and administrators for the system. There are two main screens, accessed via the tabs at the top of the screen:

- User
- Password

#### User

Click the **User** tab to access the user settings screen.

User Name	User Group
admin	Administrator

Under **User Authorization**, check **Allow anonymous viewer** to grant users who are not logged in access to the system. Click the **Save** button to confirm this setting.

Under **User List**, you can create and remove users. To create a new user, click the **Add** button. The **Add New User fields** appear. Enter a new username and password in the required fields to create a new user. Assign each user to either the admin or user groups. Click the **Save** button to save the new user. Click the **Reset** button to clear all fields. To delete a user, select the username from the User List you want to delete. Click the **Remove** button to delete the user. You cannot delete the default admin user.

#### Password

Click the **Password** tab to access the password settings screen.

Enter your username and new password. Re-confirm the new password and click the **Save** button to change the password.



#### **4.1.4 Video**

The Video submenu enables you to configure all video settings. There are two main screens, accessed via the tabs at the top of the screen:

- Video
- Audio



## Video

Click the **Video** tab to access the video settings screen.

Under **Network Traffic Control**, you can alter various options:

- **Connection Speed:** Select the High, Medium or Low radio buttons depending on the speed of your network connection.
- **Resolution:** Select the image resolution you require from the drop-down box.
- **Compression:** Select the image compression you require from the drop-down box.
- **Maximum Frame Rate:** Enter the maximum frame rate you require.
- **P-Frame / I-Frame Ratio:** Select the P-Frame / I -Frame ration you require from the drop-down box.

**Video** **Audio**

## Network Traffic Control ( from camera to computer )

- ☐ High ( more than 1.5 Mbps, LAN, Inside House )
- ☐ Medium ( 512 Kbps ~ 1.5 Mbps, LAN with many cameras )
- ☒ Low ( less than 512 Kbps, Internet, DSL, Cable )

Resolution: Compression:  (Higher compression, lower traffic.)Maximal frame rate:  frames per second (1~30)P-Frame / I-Frame Ratio:  (Higher ratio, lower traffic.)Image Parameters **Default**Brightness:  -1 Contrast:  2 Saturation:  0 Hue:  -1 

- ☐ Vertical Flip
- ☐ Horizontal Flip
- ☒ Show Camera Name
- ☒ Show Time Label



## Snapshot &amp; Record

Snapshot Path  (must exist)Record Path  (must exist)Split recording file every  minutes 

Under **Image Parameters**, you can alter image output options.

Make any adjustments for brightness, contrast, saturation, and hue of the image using the + or - buttons.

Click the **Default** button to reset to the parameters to their default value.

- **Vertical Flip:** Check to flip the display image vertically.



- **Horizontal Flip:** Check to flip the display image horizontally.
- **Show Camera Name:** Check to display the camera name in the viewing window.
- **Show Time Label:** Check to display a time and date label in the viewing window.

Under **Snapshot & Record**, you can specify the folders to which you will save all snapshots and video clips. Enter the folder you wish to save your snapshots to in the **Snapshot Path** field. Enter the folder you wish to save your video clips to in the **Record Path** field. Enter the period of time after which recordings will be split in the final field. Click the **Save** button to save all changes or the **Reload** button to reset all fields and reload the page.

## Audio

Click the **Audio** tab to access the audio settings screen.

The image shows a software interface for audio settings. At the top, there are two tabs: "Video" and "Audio", with "Audio" being the active tab. Below the tabs is a header bar labeled "Audio". Underneath, there is a checkbox labeled "Enable Audio" which is checked. Below the checkbox are two settings: "Bit Rate:" with a dropdown menu showing "32" and "Kbps", and "Audio Volume:" with a dropdown menu showing "Large". At the bottom of the settings area is a "Save" button with a mouse cursor pointing at it.

Check the **Enable Audio** checkbox to turn audio on or off. When enabled, select the audio bit rate you require from the Bit Rate drop-down box. Select the volume level from the Audio Volume drop-down box. Click the button to confirm all settings.

#### 4.1.5 Video Player

The **Video Player** submenu enables you to playback and con-vert recorded video clips to different formats.



Click the **Sfogli(Browse)** button to locate the file you wish to play. Click the **Play** and the **Stop** buttons to start and stop play-back.

Click the **Transform Recording File to AVI Format** button to convert the open video clip from .av to .avi format. Check the **Transform all files in the same folder** checkbox to batch convert all files in a folder to AVI format.

Click the **Transform FTP File to JPEG Format** button to convert an FTP file to .jpeg format.



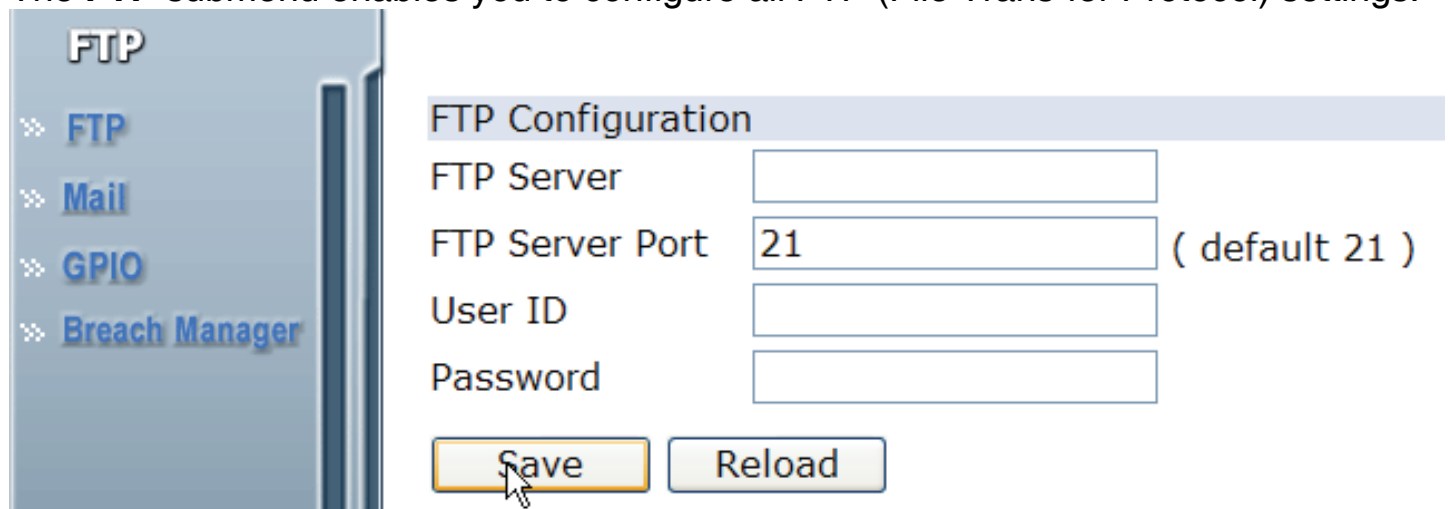
Use this function only if Motion Detection is inactive.

## 4.2 Advanced

The camera will function fine after the **Basic** configuration, however, you may wish to explore more advanced options. This section explains each parameter and setting procedures for advanced configuration of the camera. Move your mouse onto the **Advanced** button, and it will automatically pop up a submenu bar as below.

### 4.2.1 FTP

The **FTP** submenu enables you to configure all FTP (File Transfer Protocol) settings:



The screenshot shows the 'FTP' submenu on the left with options: FTP, Mail, GPIO, and Breach Manager. The 'FTP' option is selected. The main area displays the 'FTP Configuration' settings:

FTP Configuration	
FTP Server	<input type="text"/>
FTP Server Port	<input type="text" value="21"/> ( default 21 )
User ID	<input type="text"/>
Password	<input type="password"/>

At the bottom of the configuration area are two buttons: 'Save' and 'Reload'. A mouse cursor is pointing at the 'Save' button.

When FTP alerting is enabled, the camera sends a still image to the ftp server every time the alert is triggered (see “**Configuring Breach Manager Settings**” for details on how to activate this option).

Enter your FTP server and server port address, along with your username and password.

Click the **Save** button to save all changes.

### Motion Detection

- ☒ Enable Motion Detection ( Not Triggered, Latest trigger: 2006-11-27 12:47:36 )
  - ☐ Send e-mail.
  - ☒ Send images to FTP server.
  - ☐ Trigger GPIO output.



All upload files on FTP are in .AV format.

In order to convert in JPEG please check section 4.1.5 in this manual.





#### 4.2.2 Mail

The **Mail** submenu enables you to configure all mail server set-tings:

**Mail**

- ❖ FTP
- ❖ **Mail**
- ❖ GPIO
- ❖ Breach Manager

**E-Mail Configuration**

Mail Server

Mail Sender

Mail Receiver

SMTP Authentication ☐ Yes ☒ No

User Name

Password

When mail alerting is enabled, the camera sends a still image to a specified email address every time the alert is triggered (see “**Configuring Breach Manager Settings**” for details on how to activate this option).

Enter your mail server address, mail sender address, and mail receiver address. Check the radio buttons to enable notification via SMTP and enter your username and password.

Click the **Save** button to save all changes.

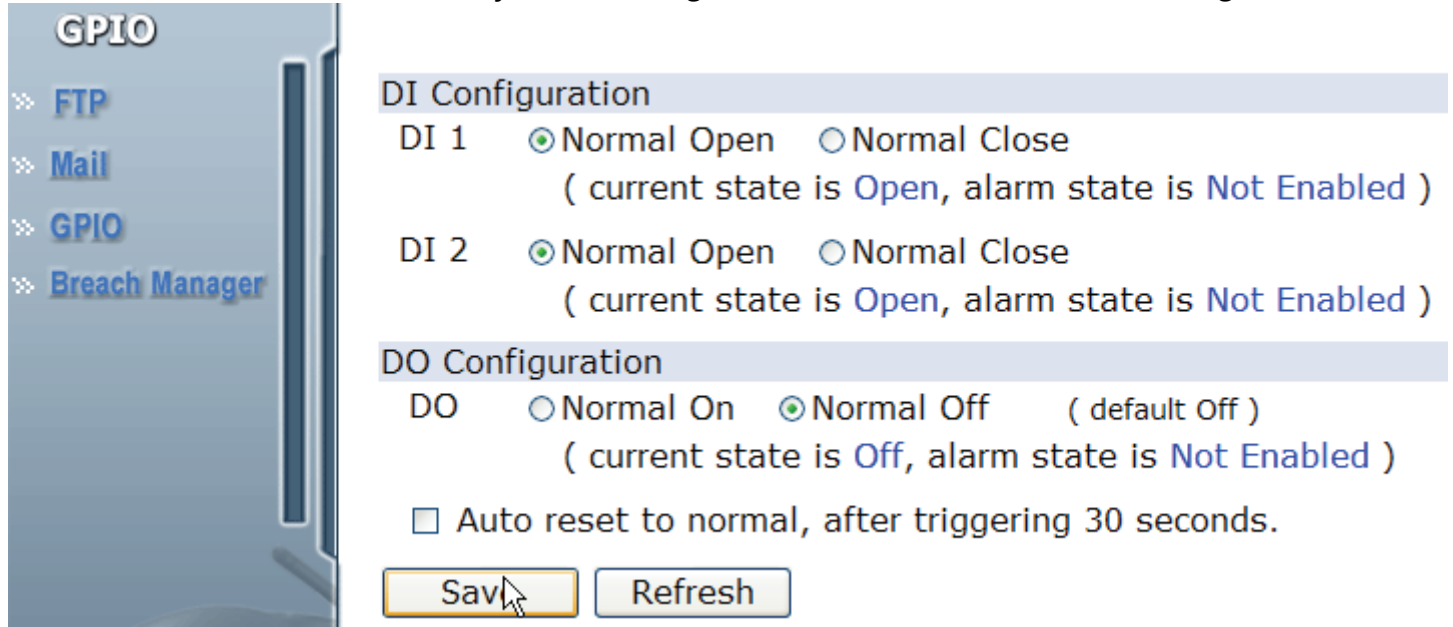
**Motion Detection**

☒ Enable Motion Detection ( **Not Triggered**, Latest trigger: **2006-11-27 12:47:36** )

- ☒ Send e-mail.
- ☐ Send images to FTP server.
- ☐ Trigger GPIO output.

### 4.2.3 GPIO

The **GPIO** submenu enables you to configure all DI sensor and DO settings:



**GPIO**

- » FTP
- » Mail
- » **GPIO**
- » Breach Manager

**DI Configuration**

DI 1 ☒ Normal Open ☐ Normal Close  
( current state is Open, alarm state is Not Enabled )

DI 2 ☒ Normal Open ☐ Normal Close  
( current state is Open, alarm state is Not Enabled )

**DO Configuration**

DO ☐ Normal On ☒ Normal Off ( default Off )  
( current state is Off, alarm state is Not Enabled )

☐ Auto reset to normal, after triggering 30 seconds.

**Save** **Refresh**

External DI sensors can be attached via the GPIO port at the rear of the camera. The external sensor can be normally open, or normally closed. A normally open sensor is like an open switch that closes when triggered. A normally closed sensor is like a closed switch that opens when triggered. This must be set correctly for an external sensor to function properly. You can connect up to two DI sensors to the camera.

An external DO alarm can also be attached to the camera via the GPIO port at the rear of the camera.

Under **DI Configuration**, select **Normal Open** or **Normal Close** for each DI1 and DI2. Click the **Save** button to confirm all settings.

Under **DO Configuration**, select **Normal On** or **Normal Off** for the DO alarm.

Check the **Auto Reset to Normal, after triggering 30 seconds** checkbox to automatically reset the alarm 30 seconds after it is triggered.

Click the **Save** button to confirm all settings and the **Refresh** button to update the page.



#### 4.2.4 Breach Manager

The **Breach Manager** submenu enables you to configure all breach alert and motion detection settings:

##### Motion Detection

- ☒ Enable Motion Detection ( **Not Triggered**, Latest trigger: **2006-11-27 12:56:55** )
- ☐ Send e-mail.
  - ☒ Send images to FTP server.
  - ☐ Trigger GPIO output.

##### GPIO DI

- ☐ Enable DI 1 ( **Not Enabled**, Latest trigger: )
- ☐ Send e-mail.
  - ☐ Send images to FTP server.
  - ☐ Trigger GPIO output.
  - ☐ Enable motion detection, if it is not enabled.
- ☐ Enable DI 2 ( **Not Enabled**, Latest trigger: )
- ☐ Send e-mail.
  - ☐ Send images to FTP server.
  - ☐ Trigger GPIO output.
  - ☐ Enable motion detection, if it is not enabled.

You can configure the system to capture images when either the motion sensors, DI1 or DI2 sensors are activated.

To set a breach alert, do the following:

Select the alert trigger device type by checking the **Enable** checkboxes next to each device.

Select the notification method from the list of options:

- **Send e-mail:** The system will send you an email when the device is triggered.
- **Send images to FTP server :** The system will send captured images to the FTP server when the device is triggered.
- **Trigger GPIO output :** The system will send a signal to the alarm devices.



- **Enable motion detection, if it is not enabled:** The system will automatically enable motion detection when the device is triggered.



## Chapter 5

### Support

#### 5.1 Support

If you have any problems with the IP Wireless Night Vision Camera, please consult this manual.

If you have any other questions you can contact the Atlantis Land company directly at the following address:

**Atlantis Land SpA**  
**Viale De Gasperi, 122**  
**20017 Mazzo di Rho(MI)**  
**Tel: +39. 02.93906085, +39. 02.93907634(help desk)**  
**Fax: +39. 02.93906161**

Email: [info@atlantis-land.com](mailto:info@atlantis-land.com) or [tecnici@atlantis-land.com](mailto:tecnici@atlantis-land.com)  
WWW: <http://www.atlantis-land.com>

## APPENDIX A: Frequently Asked Questions

### A.1 Using LEDs to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

#### A.1.1 LED Power

The PWR LED on the front panel does not light up.

Steps	CORRECTIVE ACTION
1	Make sure that the NetCamera NVW's power adaptor is connected to the Access Point and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that the NetCamera NVW and the power source are both turned on and the NetCamera NVW is receiving sufficient power.
3	If the error persists, you may have a hardware problem. In this case, you should contact Atlantis Land SpA.

#### A.1.2 LED LAN

The LAN LED on the front panel does not light up.

Steps	CORRECTIVE ACTION
1	Check the Ethernet cable connections between the NetCamera NVW and the computer or hub.
2	Check for faulty Ethernet cables.
3	Make sure your computer's Ethernet card is working properly.
4	If these steps fail to correct the problem, contact Atlantis Land SpA for assistance.



## A.2 WEB

I cannot access the web configurator.

Steps	CORRECTIVE ACTION
1	Make sure you are using the correct IP address of the NetCamera NVW. Check the IP address of the NetCamera NVW (192.168.1.1).
2	Ping the device (ping 192.168.1.1)
3	Reset the device

The web configurator does not display properly.

Steps	CORRECTIVE ACTION
1	Make sure you are using Internet Explorer 5.0 and later versions.
2	Make sure you are using Internet Explorer 5.0 and ActiveX is installed.
3	Delete the temporary web files and log in again. In Internet Explorer, click Tools, Internet Options and then click the Delete Files ... button. When a Delete Files window displays, select Delete all offline content and click OK. (Steps may vary depending on the version of your Internet browser.)

## A.3 Login

If you forget the password to log in

Steps	CORRECTIVE ACTION
1	The Reset function is to reset the setting back to factory default setting, once you press the "RESET" button within 10 seconds.
2	Before configuring this device , you need to know the following default settings: <b>Password : admin</b> <b>IP Address : 192.168.1.1</b> <b>Subnet Mask : 255.255.255.0</b>



## A.4 General Questions

Question	What is an IP Wireless Security Night Vision Camera?
Answer	The IP Wireless Security Night Vision Camera is a standalone system connecting directly to an Ethernet or Fast Ethernet network and supported by the wireless transmission based on the IEEE 802.11b/g standard. It is different from the conventional PC Camera, the IP Wireless Security Night Vision Camera is an all-in-one system with built-in CPU and web-based solutions providing a low cost solution that can transmit high quality video images for monitoring. The IP Wireless Security Night Vision Camera can be managed remotely, accessed and controlled from any PC/Notebook over the Intranet or Internet via a web browser.

Question	What is the maximum number of users that can be allowed to access the IP Wireless Security Night Vision Camera simultaneously?
Answer	Maximum number of users that can log onto the IP Wireless Security Night Vision Camera at the same time is 20. Please keep in mind the overall performance of the transmission speed will slow down when many users are logged on.

Question	What algorithm is used to compress the digital image?
Answer	The camera utilizes the MPEG-4 image compression technology providing high quality images for users. MPEG-4 is adopted since it is a standard for image compression and can be applied to various web browsers and software applications.

Question	What is the wireless transmission range for the IP Wireless Security Night Vision Camera?
Answer	Generally the wireless distance can go up to 100 meters indoors and up to 300 meters outdoors. The range is limited by the number of walls, ceilings, or other objects that the wireless signals must pass through. Typical ranges vary depends on the types of materials and background Radio





Frequency (RF) noise in your home or business and the configuration setting of your network environment.

**Question**

**Can the IP Wireless Security Night Vision Camera be used outdoors?**

**Answer**

The IP Wireless Security Night Vision Camera is not weatherproof. It needs to be equipped with a weatherproof case to be used outdoors and it is not recommended.

**Question**

**What network cabling is required for the IP Wireless Security Night Vision Camera?**

**Answer**

The IP Wireless Security Night Vision Camera uses Category 5 UTP cable allowing 10 Base-T and 100 Base-T networking.

**Question**

**Can the IP Wireless Security Night Vision Camera be setup as a PC-cam on the computer?**

**Answer**

No, the IP Wireless Security Night Vision Camera is an IP Wireless Security Night Vision Camera used only on Ethernet and Fast Ethernet network and supported by wireless transmission.

**Question**

**Can the IP Wireless Security Night Vision Camera be connected on the network if it consists of only private IP addresses?**

**Answer**

The IP Wireless Security Night Vision Camera can be connected to LAN with private IP addresses.

**Question**

**Can the IP Wireless Security Night Vision Camera be installed and work if a firewall exists on the network?**

**Answer**

If a firewall exists on the network, port 80 is open for ordinary data communication.

**Question****What is Spread Spectrum?****Answer**

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

**Question****What is DSSS? What is FHSS? And what are their differences?****Answer**

Frequency-Hopping Spread-Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.



Question	Would the information be intercepted while transmitting on air?
Answer	WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN offers the encryption function (WEP) to enhance security and access control.

Question	What is the IEEE 802.11g standard?
Answer	Approved in June, 2003 as an <a href="#">IEEE</a> standard for wireless local area networks ( <a href="#">WLANs</a> ), 802.11g offers wireless transmission over relatively short distances at up to 54 <a href="#">megabits</a> per second (Mbps) compared with the 11 megabits per second of the <a href="#">802.11b</a> ( <a href="#">Wi-Fi</a> ) standard. Like 802.11b, 802.11g operates in the 2.4 <a href="#">GHz</a> range and is thus compatible with it.

Question	What is WEP?
Answer	WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.

Question	What is infrastructure mode?
Answer	When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a wired network through a wireless access point.

Question	What is ISM band?
Answer	The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around



the globe.

**APPENDIX B: Trouble Shooting**

This chapter covers potential problems and the corresponding remedies.

Question	I cannot access the IP Wireless Security Night Vision Camera from a web browser.
Answer	<p>The possible cause might be the IP Address for the IP Wireless Security Night Vision Camera is already being used by another device. To correct the possible problem, you need to first disconnect the IP Wireless Security Night Vision Camera from the network. Then run the PING utility.</p> <p>The PING (Packet Internet Groper) command can determine whether a specific IP address is accessible by sending a packet to the specific address and waiting for a reply. It can also provide a very useful tool to confirm if the IP address conflicts with the camera over the network.</p> <p>Follow the step-by-step procedure below to utilize the PING command. However, you must disconnect the camera from the network first.</p> <p>Start a DOS window.</p> <p>Type <b>ping x.x.x.x</b>, where x.x.x.x is the IP address of the camera.</p> <p>The succeeding replies as illustrated below will provide useful explanation to the cause of the problem with the camera IP address.</p>

Question	I cannot access the IP Wireless Security Night Vision Camera from a web browser.
Answer	<p>Another possible reason is the IP Address is located on a different subnet. To fix the problem, run the PING utility. If the utility returns “no response” or similar, the finding is probably correct, then you should proceed as follows:-</p> <p>In Windows 95/98/2000 and Windows NT, double check the IP</p>



Address of the IP Wireless Security Night Vision Camera is within the same subnet as your workstation.

Click “Start”, “Setting”, “Control Panel”, and the “Network” icon. Select TCP/IP from the “Network” dialog box and from the “TCP/IP Properties” dialog box click “Specify an IP address”. If the IP Wireless Security Night Vision Camera is situated on a different subnet than your workstation, you will not be able to set the IP address from this workstation. To verify make sure the first 3 sections of the IP address of the IP Wireless Security Night Vision Camera corresponds to the first 3 sections of the workstation. Therefore the IP address of the IP Wireless Security Night Vision Camera must be set from a workstation on the same subnet.

Question	I cannot access the IP Wireless Security Night Vision Camera from a web browser.
Answer	Other possible problems might be due to the network cable. Try replacing your network cable. Test the network interface of the product by connecting a local computer to the unit, utilizing a standard Crossover (hub to hub) Cable. If the problem is not solved the IP Wireless Security Night Vision Camera might be faulty.

Question	Why does the Power LED not light up constantly?
Answer	The power supply used might be at fault. Confirm that you are using the provided power supply DC 5V for the IP Wireless Security Night Vision Camera and verify that the power supply is well connected.

Question	Why does the Link LED not light up properly?
Answer	<ul style="list-style-type: none"> <li>There might be a problem with the network cable. To confirm that the cables are working, PING the address of a know device on the network. If the cabling is OK and your network is reachable, you should receive a reply similar to the following (...bytes = 32 time = 2 ms).</li> <li>The network device utilized by the IP Wireless Security Night Vision Camera is not functioning properly such as hubs or switches. Confirm the power for the devices are well connected and functioning.</li> </ul> <p>The wireless connection might be at fault. In ad-hoc mode make sure the IP Wireless Security Night Vision Camera wireless channel and ESS-ID is set to match the PC/Notebook wireless channel and ESS-ID for direct communication. Under infrastructure mode make sure the ESS-ID on the PC/Notebook and the IP Wireless Security Night Vision Camera must match with the Access Point' s ESS-ID.</p>

Question	Why does the IP Wireless Security Night Vision Camera work locally but not externally?
Answer	<ul style="list-style-type: none"> <li>Might be caused from the firewall protection. Need to check the Internet firewall with your system administrator.</li> <li>The default router setting might be a possible reason. Need to double check if the configuration of the default router settings is required.</li> </ul>



Question	Why does a series of broad vertical white line appears through out the image?
Answer	A likely issue is that the CMOS sensor becomes overloaded when the light source is too bright such as direct exposure to sunlight or halogen light. You need to reposition the IP Wireless Security Night Vision Camera into a more shaded area immediately as this will damage the CMOS sensor.

Question	There is bad focus on the IP Wireless Security Night Vision Camera, what should be done?
Answer	You need to adjust the IP Wireless Security Night Vision Camera focus manually as described in Adjust IP Wireless Security Night Vision Camera Focus.

Question	Noisy images occur how can I solve the problem?
Answer	There might be wireless transmission interference make sure there are no other wireless devices on the network that will affect the wireless transmission.

Question	There is poor image quality, how can I improve the image?
Answer	<ul style="list-style-type: none"><li>• A probable cause might be the incorrect display properties configuration for your desktop. You need to open the Display Properties on your desktop and configure your display to show at least 65'000 colors for example at least 16-bit.</li><li>• Applying only 16 or 256 colors on your computer will produce dithering artifacts in the image.</li><li>• The configuration on the IP Wireless Security Night</li></ul>





Vision Camera image display is incorrect. Through the Web Configuration Image section you need to adjust the image related parameter for improve images such as brightness, contrast, hue and light frequency. Please refer to the Web Configuration section for detail information.

**Question**

**There are no images available through the web browser?**

**Answer**

The ActiveX might be disabled. If you are viewing the images from Internet Explorer make sure ActiveX has been enabled in the Internet Options menu.

**Question**

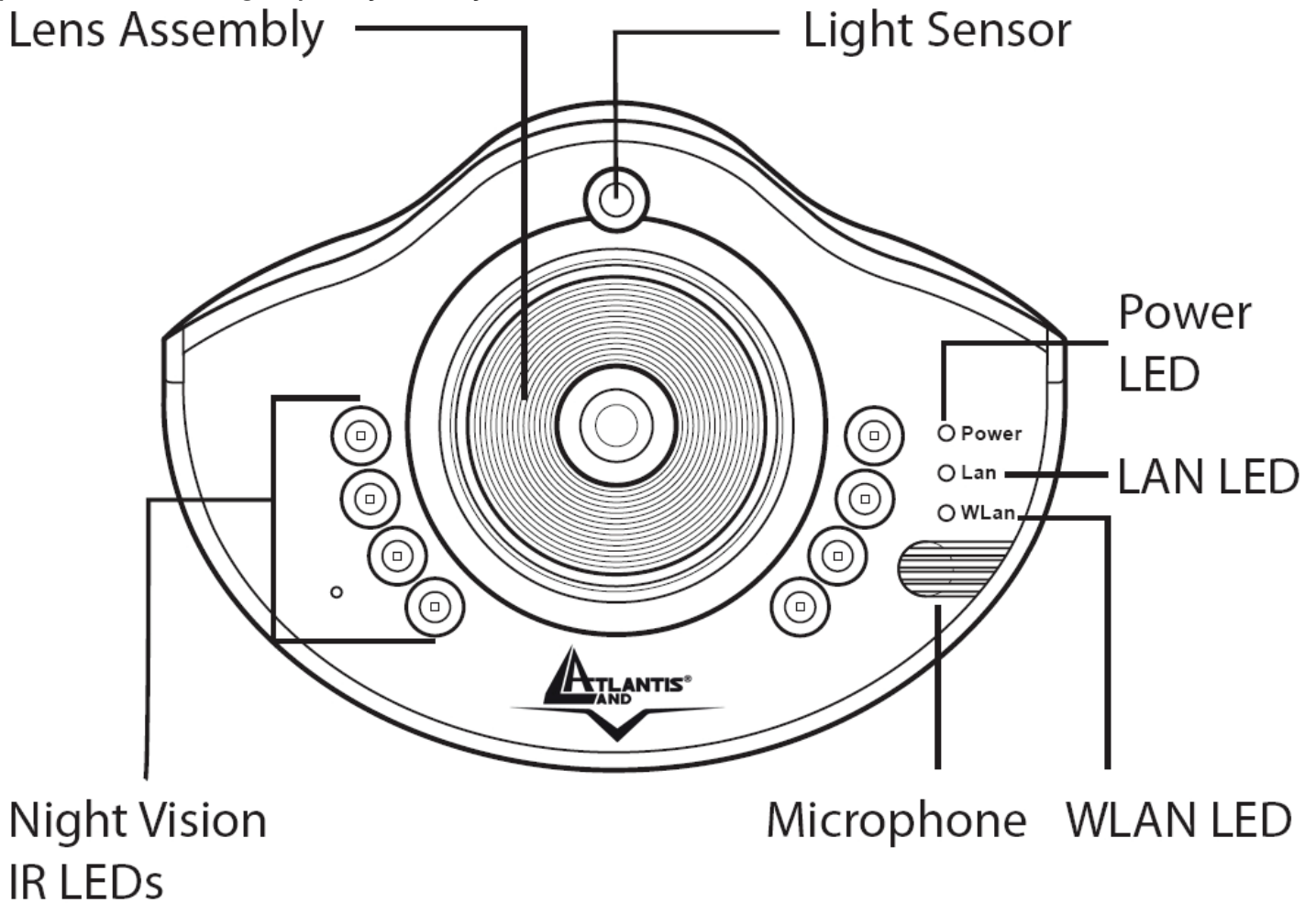
**Can I capture still images from the NetCamera NVW?**

**Answer**

Yes you are able to capture still images with the snapshot function directly into web server integrated into NetCamera NVW. Please refer to section 3.3.

## APPENDIX C: Adjusting the Camera Focus

To help you get the best image quality, keep in mind that while adjusting the NetCamera NVW (Adjust by turning clockwise or counter-clockwise )focus you can preview the image quality from your Web browser.



You can further adjust the image quality through the Web Configuration under Setup->Basic->Video. Please refer to section 4.1.4 for further details.



Direct exposure to sunlight may cause permanent damage to the device. Therefore do not expose the Internet Camera's lens directly to sunlight. The NetCamera NVW is designed for indoor usage.



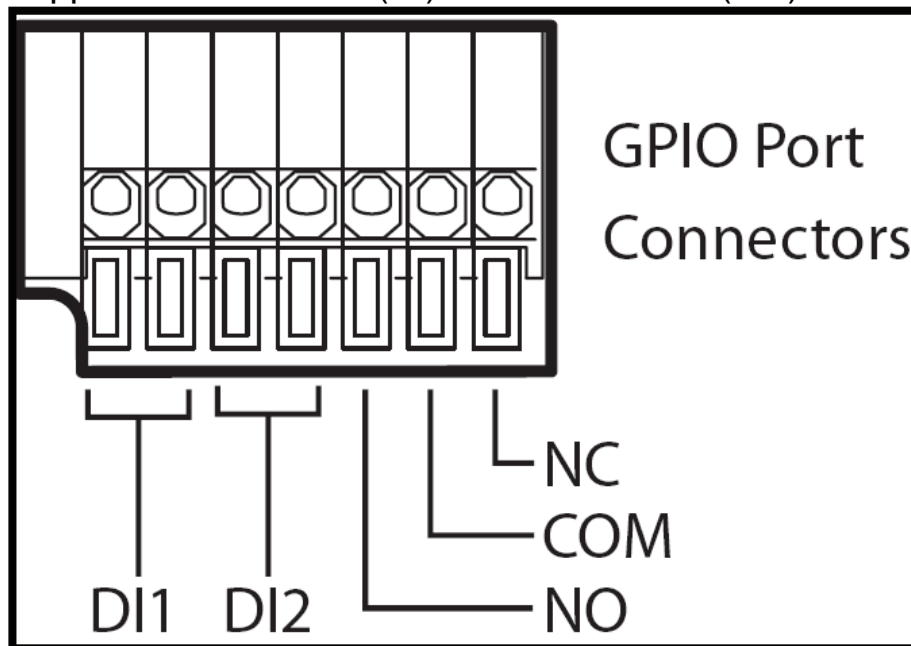
## APPENDIX D: GPIO

Its back panel contains 3 pairs of connectors (2 input and 1 output) allowing the camera to communicate with different elements of a building, such as electric doors and light switches or security related devices such as alarms.

Most of its applications are security. Warnings to the one break into house/building.

Some people use it to setting fire alarms.

NetCamera NV supports 2 sensors in (DI) and 1 alarm out (DO).







External DI sensors can be attached via the GPIO port at the rear of the camera. The external sensor can be normally open, or normally closed. A normally open sensor (NO/COM) is like an open switch that closes when triggered. A normally closed sensor (NC/COM) is like a closed switch that opens when triggered. This must be set correctly for an external sensor to function properly. You can connect up to two DI sensors to the camera.

An external DO alarm can also be attached to the camera via the GPIO port at the rear of the camera.

Under **DI Configuration**, select **Normal Open** or **Normal Close** for each DI1 and DI2. Click the **Submit** button to confirm all settings.

Under **DO Configuration**, select **Normal Open** or **Normal Close** for the DO alarm. Click the **Submit** button to confirm all settings.

NO-normal opened	Triggered
	
NC-normal closed	Triggered
	

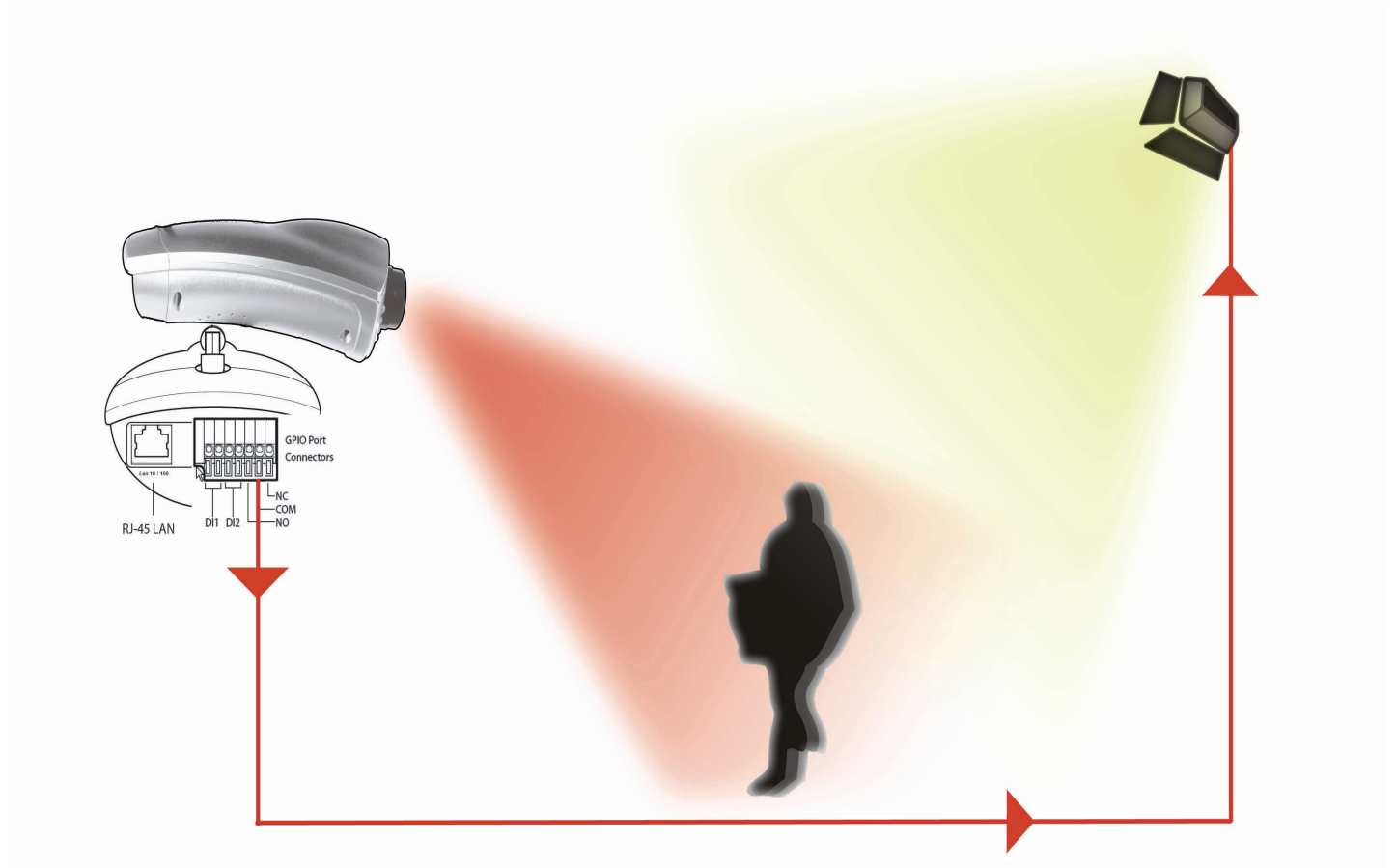


A normally open sensor (NO/COM ) is like an open switch that closes when triggered. In this case the Motion Detection switch on a spot.

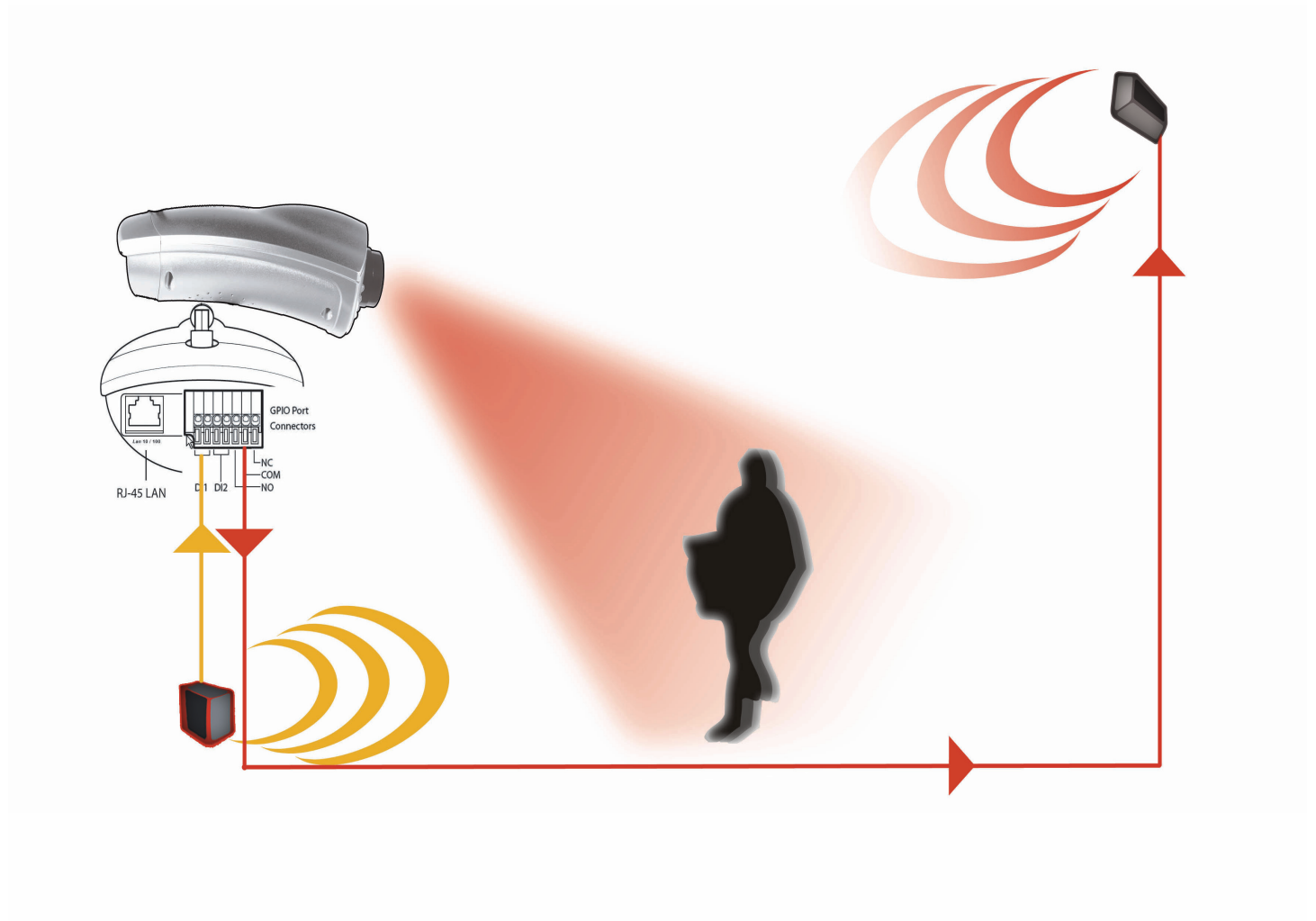


Please check the maximum Voltage/Ampere (DO):  
Max 24VDC/1A  
Max 125VAC /0.5A

For example, entrance guarding (DO)



For example, entrance guarding (DO and DI)









## APPENDIX E: Glossary of Terms

### NUMBERS

<b>10BASE-T</b>	10BASE-T is Ethernet over UTP Category III,IV, or V unshielded twisted-pair media.
<b>100BASE-TX</b>	The two-pair twisted-media implementation of 100BASE-T is called <i>100BASE-TX</i> .
<b>802.11g</b>	An IEEE standard for wireless local area networks. It offers transmissions speeds at up to 54 Mbps in the 2.4-GHz band.

### **A**

<b>Access point</b>	It is the hardware interface between a wireless LAN and a wired LAN. The access point attaches to the wired LAN through an Ethernet connection.
<b>Applet</b>	Applets are small Java programs that can be embedded in an HTML page. The rule at the moment is that an applet can only make an Internet connection to the computer from that the applet was sent.
<b>ASCII</b>	American Standard Code For Information Interchange, it is the standard method for encoding characters as 8-bit sequences of binary numbers, allowing a maximum of 256 characters.
<b>ARP</b>	Address Resolution Protocol. ARP is a protocol that resides at the TCP/IP Internet layer that delivers data on the same network by translating an IP address to a physical address.
<b>AVI</b>	Audio Video Interleave, it is a Windows platform audio and video file format.



## B

### **BOOTP**

Bootstrap Protocol is an Internet protocol that can automatically configure a network device in a diskless workstation to give its own IP address.

## C

### **Communication**

Communication has four components: sender, receiver, message, and medium. In networks, devices and application tasks and processes communicate messages to each other over media. They represent the sender and receivers. The data they send is the message. The cabling or transmission method they use is the medium.

### **Connection**

In networking, two devices establish a connection to communicate with each other.

## D

### **DHCP**

Dynamic Host Configuration Protocol was developed by Microsoft as a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. This simplifies the task for network administrators because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means a new computer can be added to a network without the hassle of manually assigning it a unique IP address. DHCP allows the specification for the service provided by a router, gateway, or other network device that automatically assigns an IP address to any device that requests one.



## DNS

Domain Name System is an Internet service that translates domain names into IP addresses. Since domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses every time you use a domain name the DNS will translate the name into the corresponding IP address. For example, the domain name *www.network\_camera.com* might translate to *192.167.222.8*.

## E

**Enterprise network** An enterprise network consists of collections of networks connected to each other over a geographically dispersed area. The enterprise network serves the needs of a widely distributed company and operates the company's mission-critical applications.

## Ethernet

The most popular LAN communication technology. There are a variety of types of Ethernet, including 10 Mbps (traditional Ethernet), 100 Mbps (Fast Ethernet), and 1,000 Mbps (Gigabit Ethernet). Most Ethernet networks use Category 5 cabling to carry information, in the form of electrical signals, between devices. Ethernet is an implementation of CSMA/CD that operates in a bus or star topology.

## F

### Fast Ethernet

Fast Ethernet, also called 100BASE-T, operates at 10 or 100Mbps per second over UTP, STP, or fiber-optic media.

### Firewall

Firewall is considered the first line of defense in protecting private information. For better security, data can be encrypted. A system designed to prevent unauthorized access to or from a private network. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially Intranets all messages entering or leaving the



intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

## G

### **Gateway**

A gateway links computers that use different data formats together.

### **Group**

Groups consist of several user machines that have similar characteristics such as being in the same department.

## H

### **HEX**

Short for hexadecimal refers to the base-16 number system, which consists of 16 unique symbols: the numbers 0 to 9 and the letters A to F. For example, the decimal number 15 is represented as F in the hexadecimal numbering system. The hexadecimal system is useful because it can represent every byte (8 bits) as two consecutive hexadecimal digits. It is easier for humans to read hexadecimal numbers than binary numbers.

## I

### **IEEE**

Institute of Electrical and Electronic Engineers.

### **Intranet**

This is a private network, inside an organization or company, that uses the same software you will find on the public Internet. The only difference is that an Intranet is used for internal usage only.

### **Internet**

The Internet is a globally linked system of computers that are logically connected based on the Internet Protocol (IP). The Internet provides different ways to access private and public information worldwide.

### **Internet address**

To participate in Internet communications and on Internet Protocol-based networks, a node must have an Internet address that identifies it to the other nodes. All Internet addresses are IP



addresses

## **IP**

Internet Protocol is the standard that describes the layout of the basic unit of information on the Internet (the *packet*) and also details the numerical addressing format used to route the information. Your Internet service provider controls the IP address of any device it connects to the Internet. The IP addresses in your network must conform to IP addressing rules. In smaller LANs, most people will allow the DHCP function of a router or gateway to assign the IP addresses on internal networks.

## **IP address**

IP address is a 32-binary digit number that identifies each sender or receiver of information that is sent in packets across the Internet. For example 80.80.80.69 is an IP address, it is the closest thing the Internet has to telephone numbers. When you “call” that number, using any connection methods, you get connected to the computer that “owns” that IP address.

## **ISP**

Internet Service Provider, is a company that maintains a network that is linked to the Internet by way of a dedicated communication line. An ISP offers the use of its dedicated communication lines to companies or individuals who can't afford the high monthly cost for a direct connection.

## **J**

## **JAVA**

Java is a programming language that is specially designed for writing programs that can be safely downloaded to your computer through the Internet without the fear of viruses. It is an object-oriented multi-thread programming best for creating applets and applications for the Internet, Intranet and other complex, distributed network.

## **L**



<b>LAN</b>	Local Area Network a computer network that spans a relatively small area sharing common resources. Most LANs are confined to a single building or group of buildings.
<b>N</b>	
<b>NAT</b>	Network Address Translator generally applied by a router, that makes many different IP addresses on an internal network appear to the Internet as a single address. For routing messages properly within your network, each device requires a unique IP address. But the addresses may not be valid outside your network. NAT solves the problem. When devices within your network request information from the Internet, the requests are forwarded to the Internet under the router's IP address. NAT distributes the responses to the proper IP addresses within your network.
<b>Network</b>	<p>A network consists of a collection of two or more devices, people, or components that communicate with each other over physical or virtual media. The most common types of network are:</p> <p><b>LAN</b> – (local area network): Computers are in close distance to one another. They are usually in the same office space, room, or building.</p> <p><b>WAN</b> – (wide area network): The computers are in different geographic locations and are connected by telephone lines or radio waves.</p>
<b>NWay Protocol</b>	A network protocol that can automatically negotiate the highest possible transmission speed between two devices.
<b>P</b>	
<b>PING</b>	Packet Internet Groper, a utility used to determine whether a specific IP address is accessible. It functions by sending a packet to the specified address and waits for a reply. It is primarily used



to troubleshoot Internet connections.

## **PPPoE**

Point-to-Point Protocol over Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as DSL or cable modem. All the users over the Ethernet share a common connection.

## **Protocol**

Communication on the network is governed by sets of rules called protocols. Protocols provide the guidelines devices use to communicate with each other, and thus they have different functions. Some protocols are responsible for formatting and presenting and presenting data that will be transferred from file server memory to the file server's net work adapter Others are responsible for filtering information between networks and forwarding data to its destination. Still other protocols dictate how data is transferred across the medium, and how servers respond to workstation requests and vice versa. Common network protocols responsible for the presentation and formatting of data for a network operating system are the Internetwork Packet Exchange (IPX) protocol or the Internet Protocol (IP). Protocols that dictate the format of data for transferors the medium include token-passing and Carrier Sense Multiple Access with Collision Detection (CSMA/CD),implemented as token-ring, ARCNET, FDDI, or Ethernet. The Router Information Protocol (RIP),a part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, forwards packets from one network to another using the same network protocol.

## **R**

### **RARP**

Reverse Address Resolution Protocol, a TCP/IP protocol that allows a physical address, such as an Ethernet address, to be translated into an IP address.

### **RJ-45**

**RJ-45 connector is used for Ethernet cable connections.**

### **Router**

A router is the network software or hardware entity charged with



routing packets between networks.

## S

<b>Server</b>	It is a simple computer that provides resources, such as files or other information.
<b>SMTP</b>	The Simple Mail Transfer Protocol is used for Internet mail.
<b>SNMP</b>	Simple Network Management Protocol. SNMP was designed to provide a common foundation for managing network devices.
<b>Station</b>	In LANs, a station consists of a device that can communicate data on the network. In FDDI, a station includes both physical nodes and addressable logical devices. Workstations, single-attach stations, dual-attach stations, and concentrators are FDDI stations.
<b>Subnet mask</b>	In TCP/IP, the bits used to create the subnet are called the subnet mask.

## T

<b>(TCP/IP)</b>	Transmission Control Protocol/Internet Protocol is a widely used transport protocol that connects diverse computers of various transmission methods. It was developed by the Department of Defense to connect different computer types and led to the development of the Internet.
<b>Transceiver</b>	A transceiver joins two network segments together. Transceivers can also be used to join a segment that uses one medium to a segment that uses a different medium. On a 10BASE-5 network, the transceiver connects the network adapter or other network device to the medium. Transceivers also can be used on 10BASE-2 or 10BASE-T networks to attach devices with AUI ports.





## U

- UDP** The User Datagram Protocol is a connectionless protocol that resides above IP in the TCP/IP suite
- ULP** The upper-layer protocol refers to Application Layer protocols such as FTP,SNMP, and SMTP.
- User Name** The USERNAME is the unique name assigned to each person who has access to the LAN.
- Utility** It is a program that performs a specific task.
- UTP** Unshielded twisted-pair. UTP is a form of cable used by all access methods. It consists of several pairs of wires enclosed in an unshielded sheath.

## W

- WAN** Wide-Area Network. A wide-area network consists of groups of interconnected computers that are separated by a wide distance and communicate with each other via common carrier telecommunication techniques.
- Windows** Windows is a graphical user interface for workstations that use DOS.
- Workgroup** A workgroup is a group of users who are physically located together and connected to the same LAN, or a group of users who are scattered throughout an organization but are logically connected by work and are connected to the same network group.
- Workstations** Workstation refers to the intelligent computer on the user's desktop. This computer may be an Intel-based PC, a Macintosh, or a UNIX-based workstation. The workstation is any intelligent device a user works from.



## APPENDIX F: Technical Features

### TECHNICAL FEATURES

#### CMOS Sensor

Number of effective pixels: 307200 pixels (VGA)

Resolution: 640 x 480 pixel

Lens Type: C3 Mount Lens (removable)

Focal length: f=6.0mm

F-number: F1.8

Focus Extent: 20 cm -  $\infty$

#### Image (Video Setting)

Image compression: MPEG4

Frame rate: 30fps@QVGA, 30fps@VGA

Compression Rate selection: 5 levels

Video resolution: 320x240, 640x480

Upside down and Mirror: Yes

Brightness/ Contrast /Saturation/HUE

Night Vision: 8 x IR LEDs (auto/manual)

#### Audio

MIC Input: Internal MIC (mono)

Audio Compression: ADPCM 16/24/32/40 Kbit

#### Hardware Interface

LAN Connector: One RJ-45 port to connect to 10/100Mbps Ethernet, auto-sensed

WLAN: one 2.2 dBi Antenna built-In (IEEE802.11g with WEP 65/128 and WPA\* support)

LED Indicator: Power LED, LAN, Wlan

Power Supply: DC 5V, switching type

GPIO: 2 x Sensor IN / 1 x Sensor OUT

#### Communication Support

Communication: 10/100Mbps Ethernet

Communication protocol: HTTP, TCP/IP, UDP, ARP, ICMP, DHCP, PPPoE, DDNS, DNS, FTP



## **System**

CPU: ARM9/MPEG4 encode chip (VGA)

## **System Requirements**

Local Area Network: 10Base-T Ethernet or 100Base TX Fast Ethernet

CPU: Intel Celeron 1.5GHz or above (Intel Pentium 4 is preferred)

Memory Size: 128 MB (256 MB recommended)

VGA card resolution: 800x600 or above

Internet Explorer 5.0 or above (ActiveX)

## **Advanced Features**

MPEG4 encode Chip

Hardware motion detection and send e-mail (with snap shot) when motion detected

GPIO: Sensor IN, Alarm Out

Single Frame Image Snap shot (manual)

Record (AVI, manual)

FTP / PPPoE / Dynamic DNS Clients

## **Operating environment**

Operating temperature: 5°C ~ 30°C

Storage temperature: -25°C ~ 50°C

Humidity: 20% ~ 80% non-condensing

## **Package Contents:**

One IP Security Wireless Night Vision Camera

One Quick Installation Guide

One Installation CD Rom

One Metal Clip (wall mounting)

One DC Power Adapter

One RJ-45 Ethernet Cable

All rights registered

Microsoft and Windows are registered trademarks of Microsoft Corporation

All trade names and marks are registered trademarks of respective companies

Specifications are subjected to change without prior notice. No liability for technical errors and/or omissions

Performance and Throughput are influenced by many factors (interference, noise, environments)



\*available with new firmware release



**Atlantis Land S.p.A.**  
**Viale De Gasperi, 122**  
**Mazzo di Rho – MI – Italy**  
[info@atlantis-land.com](mailto:info@atlantis-land.com)  
[sales@atlantis-land.com](mailto:sales@atlantis-land.com)

---

**Where solutions begin**